FEATS OF STRENGTH

A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE

Future-Proof Leadership

Building Programs and People That Stand the Test of Time

Featuring:

Jeff Spear, CISO, Tufin
Kyle Thomas, Sr Director Global InfoSec, Wex
Lisa Lafleur, Director, External Party Risk Management, Walmart
Michael Brewer, CISO, Neurocrine Biosciences
Rose Lally, CISO, Altisource
Sean Dobson, CISO & CTO, Wafra
Yash Murali, CTO, Therabody

DECEMBER 2025

K logix

TABLE OF CONTENTS

FEATURES

December 2025

MAGAZINE CONTRIBUTORS

Katie Haug - Editor in Chief
VP Marketing, K logix

Kevin West - Editor
CEO, K logix

Emily Graumann - Graphics
Graphic Designer, K logix

ABOUT K LOGIX

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication Feats of Strength. Through hundreds of CISO interviews, we extract trends in order to provide services that align business to information security.

DEAR READERS,

In this issue of Feats of Strength, we explore what it means to be a future-proof leader in a time of constant change. Every leader featured in these pages has navigated a landscape shaped by new technologies, evolving risks, and rising expectations. Yet what stands out is not the pace of innovation, but the steady commitment to people, communication, and purpose. Their stories remind us that true resilience does not begin with tools. It begins with mindset.

Across our conversations, leaders spoke openly about the opportunities and challenges ahead, especially as artificial intelligence becomes part of everyday work. But beneath the surface, a larger theme emerges. Future proof leaders are defined not by the technology they adopt, but by the clarity they bring to complexity and the trust they build within their teams. They listen, they adapt, and they empower others to grow alongside them. These pages highlight that leadership is not about predicting the future, but preparing people to thrive in it.

We hope this issue inspires you as much as these leaders inspired us. Their journeys show that the most enduring strength comes from curiosity, communication, and a willingness to evolve. As the security landscape shifts, the future belongs to those who lead with intention — and who see change not as a disruption, but as an invitation to rise.

- Katie Haug, Editor in Chief

Future Proof Leadership:

What Security Leaders Need Now

By Katie Haug

Across conversations with cybersecurity leaders featured in Feats of Strength, one message is unmistakably clear: the future will not reward those who stand still. It will belong to leaders who adapt, learn, unlearn, and lead with clarity in a world defined by rapid technological change.

Artificial intelligence may be the most visible force shaping today's strategy, but true future-proof leaders see beyond tools. They understand that technology alone does not secure a business or guide a team. Instead, it is the leader's mindset, communication style, culture building, and vision that determine whether an organization thrives in the years ahead.

In our latest set of interviews, 100 percent of security leaders mentioned AI, and 75 percent identified it as one of their top strategic priorities. But when you listen closely, what emerges is not an AI story. It is a leadership story, one about adaptability, clarity, and the ability to create structure amid uncertainty.

The future-proof leader is not a technologist. They are a strategist. An enabler. A communicator. And above all, a guide.

THE HUMAN CENTER OF FUTURE-PROOF LEADERSHIP

While AI was mentioned in every interview across this year's Feats of Strength profiles, leaders consistently emphasized the primacy of people.

On page 11, Lisa Lafleur, Director of External Party Risk Management at Walmart, grounds her leadership philosophy in transparency and empathy. "My job is to empower the people around me to reach their full potential," she says. "I tell my team all the time: my job is to get obstacles out of your way."

Her words reflect a universal shift: future-proof leadership is people-first. Tools and technologies change. Human motivation, trust, and purpose remain at the center of great leadership.

Kyle Thomas at WEX echoes this mindset on page 8. "If I have to do someone's job for them, I am either overpaying or I am not doing my job," he says. His focus on developing leaders rather than followers is crucial to building teams that can navigate ambiguity. Future-proof leaders are not building dependency. They are building capability.

This emphasis on growth shows up again in Jeff Spear's philosophy at Tufin on page 6. "Security changes daily," he says. "The best thing I can do is create a culture where learning is constant and curiosity is rewarded."

In an era defined by speed, the leaders who thrive will be those who cultivate continuous learning not as a program, but as a cultural expectation.

CLARITY AND COMMUNICATION IN AN AGE OF COMPLEXITY

Across the interviews, the strongest leadership skill is not technical knowledge. It is the ability to communicate clearly, especially when explaining complex ideas to business leaders, regulators, or boards.

Sean Dobson learned early that technical excellence is not enough. "My review said I was the most technical person my boss had ever worked with, but that I needed to work on communication," he says on page 16. Today as both CISO and CTO, communication is the core of his executive presence.

Similarly, Jeff Spear recalls transitioning into leadership roles where success meant moving from deep technical detail to business relevance. His experience managing disaster recovery during major events shaped his communication style: clear, calm, and focused.

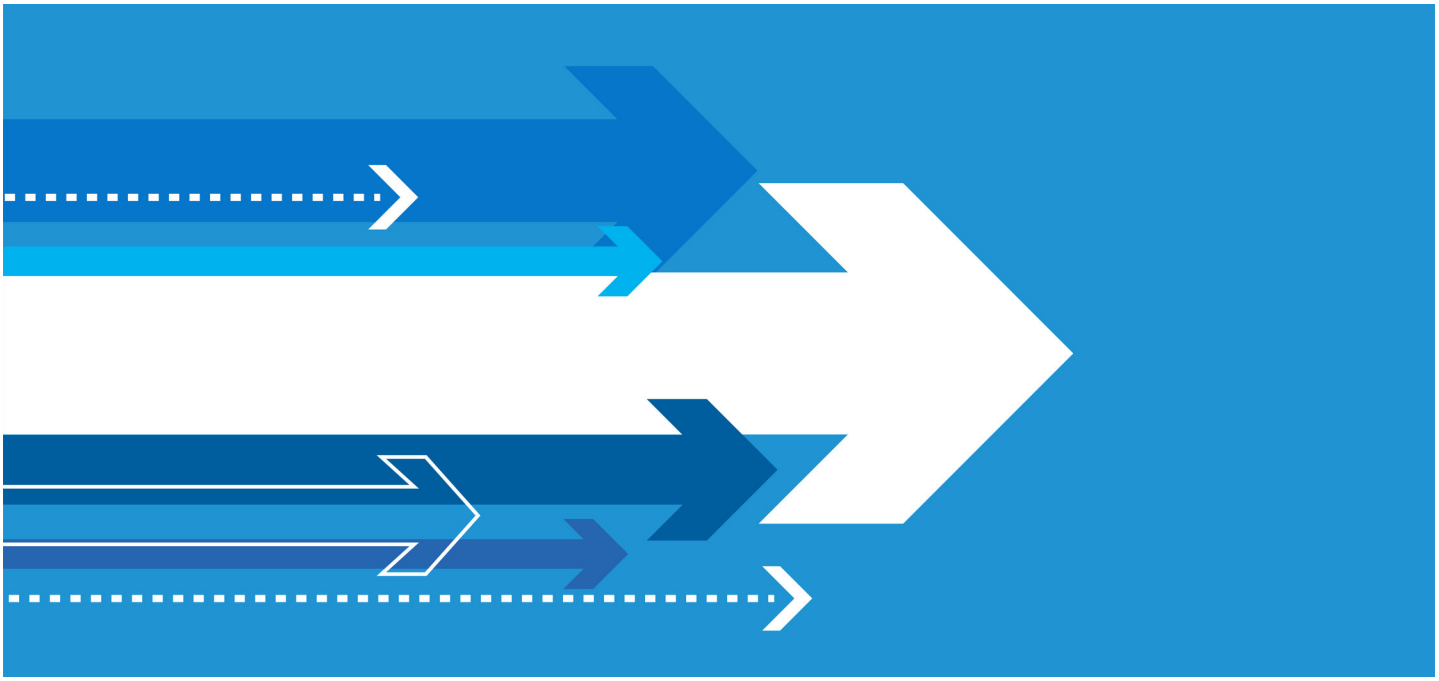
Lisa Lafleur pursued her MBA specifically for this reason. "I wanted to be able to explain what we do to the business and talk to executives in their language," she says (page 10). This ability to translate between technology and strategy is what now enables her to lead one of the most complex vendor ecosystems in the world.

And at Therabody, CTO Yash Murali embodies communication through purpose on page 18. "Data tells you what is happening," he says. "Stories tell you why it matters."

Future-proof leaders tell stories. They connect the dots for others. They make the invisible visible. They remove fear by offering clarity.

BUILDING TEAMS FOR TOMORROW

Future-proof leaders recognize that the next decade will require new capabilities. But instead of hiring for exact skill sets, which



may not exist yet, they hire for learning agility.

Michael Brewer says it simply: “I hire adults. I do not micromanage.” His trust empowers his team to innovate, adapt, and grow.

Rose invests deeply in mentorship and inclusion. “We need more women in this field,” she says. “If sharing my story helps even one person, it is worth it.”

THE FUTURE-PROOF LEADER

A future-proof leader is defined not by the technology they deploy, but by the clarity and confidence they bring to complexity.

Across our interviews, a shared set of traits emerged:

1. Curiosity: Leaders who ask questions, seek new information, and remain open to changing their minds.
2. Purpose-driven communication: Translating complexity into clarity. Explaining the “why,” not just the “what.”
3. Human-centered leadership: Seeing people as the priority, not the technology.
4. Adaptability: Navigating uncertainty with calm, learning quickly, and pivoting when needed.
5. Long-term vision: Building programs and people that stand the test of time.

These characteristics appear again and again in the leaders we interviewed, regardless of industry, program maturity, or company size.

WHAT COMES NEXT

If AI was the spark that forced leaders to look ahead, future-proof leadership is the discipline that will carry organizations forward. The next frontier is not automation or analytics. It is the evolution of the security leader.

Yash captured it best: “A future-proof leader is someone who can navigate uncertainty without losing sight of the mission.”

These leaders are proving that while technology may set the pace, leadership sets the direction. And the ones prepared for tomorrow are not those who know the most, but those who are willing to grow the fastest.

PROFILES IN *Confidence*

JEFF SPEAR

CISO
Tufin

Headquarters: Boston, MA

Employees: 500+

Annual Revenue: Private Company

Before Jeff Spear led security teams, he led teams through some literal storms. In one of the earliest moments of his career, Jeff learned how maintaining clarity and composure in a difficult situation can shape outcomes, a lesson that would later guide how he fosters teams and manages risk.

"I grew to lead our Deployment Engineering team when Superstorm Sandy hit and caused massive disruption along the east coast," Jeff recalls. "Our CISO noticed how I communicated and stayed calm under pressure and asked me to join the security team to lead disaster recovery programs for our enterprise clients. That's when I realized security combined my technical curiosity with my desire to help others understand and manage risk. That experience changed everything for me."

Since then, Jeff has built and led security programs across multiple industries, from healthcare and hospitality to financial technology. Each role taught him something new about leadership and adaptability. "I've had the opportunity to build programs from the ground up, lead through acquisitions, and help companies define what good security looks like," he says.

BUILDING A SECURITY CULTURE

Jeff views building a security culture as shaping habits and mindsets across every part of the organization, and as an extension of Tufin's mission to help enterprises develop and maintain their network security posture.

"The company's position in the security industry adds unique pressure to do security exceptionally well. If we're in the business of helping customers achieve Zero Trust through our solutions, we have to embody that internally," Jeff says.

Before accepting the role, he focused on a few key criteria. "I wanted to ensure there was an appetite to invest in people and tools," he explains. "Budget and staffing don't have to be perfect, but there has to be willingness to grow." He also prioritized executive alignment. "I met with the entire C-suite during my interviews," he says. "I wanted to make sure the 'C' in CISO meant something, that I'd have a real seat at the table."

Those conversations confirmed what Jeff hoped, that Tufin values security as a business enabler rather than an obstacle. "The culture was supportive from day one," he says. "Security is viewed as part of how the company delivers value, not just as a cost center."

SHAPING THE MODERN SECURITY PROGRAM

Jeff divides his program into four core areas: governance and compliance, security programs, application security, and security operations. Within those areas, he oversees everything from cloud and identity security to resilience and secure code development. "It's a model that's worked for me because it aligns with both product-based organizations and traditional enterprises," he explains.

Application security remains one of his biggest priorities. "We're a product organization, so secure code is everything," he says. "My focus is to make sure we can ship secure software as efficiently as possible without slowing innovation."

AI AND THE FUTURE-READY ENTERPRISE

Like many of his peers, Jeff sees artificial intelligence as both a powerful tool and an emerging challenge. "AI is top of mind for every CISO right now," he says. "For me, it's about

using AI across our security program to do more with less, while managing the risks it introduces."

When Tufin procures new technologies, AI included, security is at the center of the conversation. "We have a solid third-party risk management process that ensures security is involved in every decision," he explains. "When we licensed enterprise AI tools, I was part of the discussions with vendors, reviewing SOC 2 reports and secure development practices. It's just part of how we operate."

He also points out that the rise of AI-generated code brings new complexity. "A developer using AI can produce code one hundred times faster," he says. "That's great for productivity, but it also means we need smarter ways to review and test that code for vulnerabilities. The scale is different now."

Still, Jeff views AI as an accelerator for good. "It's about balance," he says. "AI can improve detection, automate response, and make security operations more efficient. The key is using it responsibly and transparently."

GROWTH AND LEARNING

Jeff's approach to leadership was shaped by a lesson early in his career. "One of my directors introduced me to the concept of a growth mindset, the idea that you add 'yet' to every challenge," he says. "If you don't understand something, it just means you don't understand it yet."

That perspective has stayed with him, especially in a field as dynamic as cybersecurity. "Security changes daily," he says. "The best thing I can do for my team is create a culture where learning is constant and curiosity is rewarded."

He encourages his teams to embrace challenges and remain flexible. "I tell them they don't have to know everything," he says. "What matters is their ability to adapt and find the right answers."

THE VALUE OF COMMUNITY

For Jeff, community and peer collaboration have been vital to his growth as a leader. "I wouldn't have had any of my roles if it weren't for the relationships I've built through networking," he says. He credits in-person events and conferences as valuable learning opportunities.

"The best place to network in my experience has been through in-person events, whether that's the big conferences like Black Hat, DEF CON, or RSA, or the smaller regional ones like ISC chapter meetings or SecureWorld in Boston," he says.

"I find less value in the sessions and more value in the people who are in the sessions with me," he says.

Those relationships, built on trust and shared experience, create a network of peers he can turn to when evaluating new technology or solving complex problems. "If I'm looking at a technology and I know someone who's already used it or done a proof of concept, it saves so much time. Instead of testing three different products, I might only test two because I can trust their experience," he explains.

At this stage of his career, Jeff sees his role not only as protecting systems but also as empowering people, both within Tufin and across the security community. "Security is ultimately about enabling the business to move with confidence," he says. "My job is to create an environment where teams feel supported, informed, and equipped to make good decisions."

Whether navigating literal storms early in his career or the evolving challenges of modern cybersecurity, Jeff returns to the same principles: clarity, curiosity, and connection. "If we stay adaptable, invest in our people, and continue learning from one another, we can meet any challenge ahead," he says. "That is what makes this work meaningful and what makes Tufin a place where security can truly thrive."

PROFILES IN *Confidence*

KYLE THOMAS

SENIOR DIRECTOR, GLOBAL INFORMATION SECURITY

WEX

Headquarters: Portland, ME

Employees: 6,500

Annual Revenue: $2.6 Billion

Kyle Thomas describes his path into cybersecurity as "nonlinear," yet it is precisely that diversity of experience that exemplifies his strength as a leader. His career began in the late 1990s as technology was taking shape, and he grew alongside it, earning certifications across everything from database design, to JavaScript, and firewalls. Over time, his adept curiosity led him into security leadership, where his ability to bridge technology and strategy became a defining skill.

In 2022, Kyle's career journey led him to WEX, a global commerce platform, where he took on the role of Director, then Senior Director of Global Information Security. When joining the organization, Kyle was drawn not only to the technology stack but to what he describes as a "true culture of security." "When I joined, we had roughly fifty people in security," he recalls. "That's a large number for an organization our size, but it reflected the complexity of what we do."

WEX operates across three lines of business including Mobility, Corporate Payments, and Benefits, and provides services to clients in over 200 countries. The company processed more than $200 billion in payment volume last year, managing data across 20 currencies and tens-of-millions of user accounts. "It's a global organization with a highly regulated environment," Kyle explains. "We're subject to PCI, SOX, SOC, HIPAA/HITRUST, GDPR, and numerous other global privacy frameworks. That level of maturity made me confident this was a place where security had real influence."

CULTURE OF SECURITY

Since joining WEX, Kyle's scope of responsibilities has grown significantly. Starting at two teams and 13 people, he now leads a team of 40 members across five countries, overseeing network security, data protection, identity protection, automation, and security applications. He is closely partnered with Application Security, Architecture, and GRC teams, serving on advisory boards, and working with senior technology leaders to align security with innovation.

One of his primary focuses is helping the organization balance product velocity with security oversight. "Our goal is to enable rapid experimentation and innovation while maintaining compliance and protecting data," he says. "That means staying closely connected to digital and product leadership and making security part of the business rhythm."

Each year, Kyle and his teams begin with what he calls "brag books", internal reports that track metrics, project milestones, and wins. "We aggregate those into an annual brag book and present it across the organization," he explains. "It's not just about showing numbers like the 120 million threat blocks we average per day, or the 400,000 daily container runtime scans, it's about showing what we can achieve when we work together." That transparency helps build trust and alignment across departments, reinforcing security's role as a business enabler.

AI AND THE FUTURE-READY ENTERPRISE

Kyle describes artificial intelligence as both a driving force and a challenge for the modern security leader. "AI is everyone's focus right now," he says. "We've built AI-powered tools to simplify processes, but that means our focus must include securing those models, monitoring them for vulnerabilities, and ensuring we use AI responsibly."

For WEX, the integration of AI is not only operational but also strategic. The organization continues to explore how AI can streamline operations, identify threats faster, and even

support defensive automation. “We use AI to fight fire with fire,” Kyle explains. “If threat actors are using AI, so should we.”

He notes that AI security overlaps with several other domains. “It’s similar to application and identity security. Overprivileged AI agents can create risk just like any other non-human account. It’s about managing those permissions and maintaining control.”

As part of his annual planning, Kyle focuses on short, actionable roadmaps rather than multi-year strategies. “Security evolves too fast for long-term static plans,” he says. “Three years ago, no one had AI in their strategy, and now it’s a major priority. Being future-ready means staying adaptable and focusing on measurable progress each year.”

BUILDING TRUST

To translate complex security strategies into business language, Kyle believes communication must start with “the why.” He believes in a philosophy of purpose-driven communication. “Security can’t just say no, we have to show why something matters, what the risk is, and how we can partner to solve it,” he says.

That philosophy has helped him earn the trust of executives and peers across the organization. His team conducts annual roadshows to share results, discuss upcoming initiatives, and gather feedback from product and technology leadership. “Those sessions are key,” he says. “They turn security into a shared mission instead of a separate function.”

Kyle also emphasizes a service-oriented mindset. “In security, our customers are usually internal. If a security control creates friction, our job is to guide and support, not to punish,” he explains. “Trust is built in small moments. You earn it by showing up and helping.”

LEADERSHIP WITH TRANSPARENCY

Kyle describes his leadership style as open and honest. Every new employee receives the same speech on their first day: clear expectations, candid feedback, and empowerment to take ownership. “If I have to do their job for them, I’m either overpaying or I’m not doing my job,” he says with a laugh. “My job is to create space for people to excel.”

He encourages his team to innovate and challenge convention. “We say the box is where we put our ideas when we’re done,” he notes. Each team member is required to set two annual development goals, one technical and one professional. “It’s my responsibility to develop leaders,” he says. “That means giving them room to fail safely and learn from it.”

When hiring, Kyle prioritizes cultural fit and capability over credentials. “We removed degree and certification requirements from our roles,” he explains. “Skills and mindset matter more. We can help someone earn a certification later if they have the drive and curiosity to learn.”

He believes diverse experiences strengthen the team. “We operate globally, and certifications popular in the U.S. may not carry the same weight in India or the UK. I care about competence and problem-solving. The rest can be developed.”

A LIFELONG LEARNER

Kyle practices what he teaches by setting his own development goals each year. He reads, listens to leadership podcasts, and attends industry conferences to stay current. “I’m a big believer in lifelong learning,” he says. “Every day, I try to learn something new.”

He also values the network of peers he’s built through professional events. “We all need someone to call when we hit a new challenge,” he says. “Conferences and groups give you that lifeline. You can ask, ‘Have you seen this before?’ And learn from each other.”

Looking ahead, Kyle hopes to see more collaboration across technology disciplines. “We talk a lot about breaking down silos, but we still tend to separate CISOs, CIOs, and CTOs into different circles,” he reflects. “We have so much to learn from each other. If we want to move the industry forward, we need more of those mixed conversations.”

At WEX, Kyle is leading by example, proving that future-proof leadership means more than adapting to technology. It means empowering people, communicating purpose, and building a culture of trust that stands ready for whatever comes next.

PROFILES IN *Confidence*

LISA LAFLEUR

DIRECTOR, EXTERNAL PARTY RISK MANAGEMENT

Walmart

Headquarters: Bentonville, AR

Employees: 2.1 Million

Annual Revenue: $674.5 Billion

Lisa Lafleur didn't plan a career in cybersecurity, she built one out of curiosity and conviction. "I was the first cybersecurity person at a bank I worked at during the beginning of my career," she says. "When I hired on as a network manager, I saw a need for cybersecurity and talked to my boss about it. He said, 'Do we even need cybersecurity people?' That was really the attitude at the time."

Lisa convinced him otherwise, laying the groundwork for what would become a long and distinguished career in information security. "That was my first entry into security, but there were always elements of it in my work," she explains. "I had been writing policies for ten years, and I worked in audit, doing some auditing of cybersecurity as well."

Her early years reflect the infancy of the cybersecurity industry. "When I was in audit, the main control was making sure we had power strips and we knew where the policy was," she recalls with a laugh. "Auditors would read books to figure out what they needed to ask me. They once said we needed firewalls, but we weren't even on the internet yet. I said, 'We don't need firewalls; we don't have anything to firewall off.' It was such an interesting time."

FINDING HER PLACE AT WALMART

Today, Lisa is the Director of External Party Risk Management at Walmart, a role she has held for more than four years. Her path to Walmart began long before the opportunity appeared. She spent years building a reputation in financial services, defense, and manufacturing, working in positions that exposed her to governance, audit, networking, policy writing, and eventually security leadership.

During her time at Raytheon she worked for a leader who became a long-term mentor. "The person who hired me at Raytheon hired her at Walmart. It is important to maintain your network and keep relationships going even if you change roles."

The position at Walmart offered Lisa the chance to build something new. Lisa saw the External Party Risk Management program as an opportunity to apply decades of strategy and governance experience toward a large-scale initiative. "This was my opportunity to build something meaningful and give back to the community if I could build it the right way."

LEADING A COMPLEX GLOBAL PROGRAM

Lisa's role focuses on vendors that don't supply the products on Walmart's shelves but still handle sensitive data. "Any vendor with whom we exchange protected information has to go through my team," she explains. "We look at it from two perspectives: onboarding and continuous management."

Her team ensures that every vendor meets Walmart's strict security standards before work begins. "We use NIST and other industry frameworks to make sure vendors meet our requirements," she says. "We make sure they're protecting data in the same way we would protect it in-house, with all the same or equivalent controls."

The team has full authority to reject vendors that don't meet those standards. "We absolutely have the power to say no," she says. "And so far, every decision we've made has been backed one hundred percent."

Once a vendor is approved, Lisa's team monitors them continuously. "We make sure they maintain that level using mostly OSINT data," she says. "We look for vulnerabilities on their external servers and make sure nothing's falling through the cracks."

Her group's scope extends well beyond third-party oversight. "We're not just third-party risk management; we're external party risk management," she explains. "That means we also look at fourth parties and beyond. Sometimes those fourth-party relationships pose even bigger risks to the supply chain than the third parties themselves."

AI, DATA, AND THE EXPANDING RISK LANDSCAPE

As with nearly every area of security, AI is both an opportunity and a challenge. "AI is probably the biggest change and the biggest challenge," Lisa says. "All of a sudden, everybody can code and create tools. We're going to need strong strategies and leaders to stand beside them to make sure these developments align with our goals and don't become distractions."

Her team is also exploring how AI can improve visibility into Walmart's vast vendor ecosystem. "For years, we've been collecting data on all of our vendors," she explains. "Now we're asking, how can we use that data to make better risk-informed decisions and increase the health of the ecosystem?"

Lisa sees her work as part of something much larger. "The more data we analyze, the more we realize how interconnected every company is," she says. "People joke about six degrees of separation, but in cybersecurity, it's more like two. One vendor's issue can quickly become everyone's issue."

Looking ahead, Lisa's priorities include expanding the program internationally and integrating AI responsibly. "We want to leverage AI to increase insights and efficiency, but it has to be tied to the overall strategy," she says. "And internationally, we're figuring out how to scale our processes and make sure they're built into everything we do."

TRANSLATING SECURITY INTO BUSINESS IMPACT

For Lisa, communication is as critical as technology. "That's why I got my MBA," she says. "I wanted to be able to explain what we do to the business and talk to executives in their language."

She uses an agile framework to track progress and align with corporate strategy. "We capture everything in sprints, stories, and epics," she explains. "I work with the program management office to make sure what I'm doing reads into their strategy. I meet with strategic leads all the time to explain my business cases and make sure our priorities are aligned."

That alignment with business value is essential in Walmart's culture. "At the end of the day, our job is to increase shareholder wealth," she says. "Walmart is very particular about everyday low cost or EDLC. We look at every penny because we really do care about providing the lowest costs for our customers. It all makes sense when you walk into a store and see how that strategy connects."

LEADERSHIP WITH PURPOSE AND INTEGRITY

Lisa describes herself as a servant leader, a philosophy that defines her approach to management. "My job is to empower the people around me to reach their full potential," she says. "I tell my team all the time: my job is to get obstacles out of your way."

She values transparency and open dialogue, even around difficult topics like AI. "We had an honest conversation about AI and its existential threat to some of the work we do," she says. "One of my team members told me they were surprised I brought it up. But I think talking about it makes it less scary. Avoiding it doesn't."

Her empathy and honesty create a culture of trust. "I like to be honest and always say I'm too lazy to be dishonest," she laughs. "It's just too hard. I'd rather be upfront."

Lisa also believes in giving back. "At a certain point in your career, it's important to contribute to the community," she says. "I'm active in ISC^2 and InfraGard and serve on chapter boards. I think it's especially important as a woman in this field. Young women don't always see opportunities for themselves, and sometimes they're too hard on themselves. I want to change that."

She makes time for mentorship wherever she can. "I love it when young women reach out," she says. "If I can fit it in, I'll always prioritize those conversations. We need more women in this field, and if sharing my story helps even one person, it's worth it."

BUILDING A DIVERSE AND INCLUSIVE FUTURE

Diversity and inclusion are more than talking points for Lisa, they're daily priorities. "As a leader, I think it's important to understand generational, cultural, and gender differences," she says. "Those things can become barriers if we don't take time to learn about them."

She makes a point of learning from her global team members. "I have people from Panama, Ghana, Mexico, India, and it is fascinating to learn from them," she says. "I'm constantly asking questions about where they're from and how they see things. When you understand different perspectives, it builds appreciation and teamwork."

Lisa believes that diversity strengthens security. "When you bring people with different backgrounds and experiences together, you get better ideas," she says. "That's how we build stronger teams and a stronger industry."

At Walmart, Lisa leads with humility and a deep sense of purpose. "Every day is different," she says. "There's no playbook, but that's what makes it exciting. My goal is to help my team succeed, support the business, and hopefully leave this program and this industry better than I found it."

PROFILES IN *Confidence*

MICHAEL BREWER

CISO

Neurocrine Biosciences

Headquarters: San Diego, CA

Employees: 2,500+

Annual Revenue: $2.36 Billion

Michael Brewer's journey into cybersecurity began in the U.S. Army, where his career quickly evolved from running telephone lines to building complex network systems. He shares, "Networking was just starting to become something the Army was going to use for their forward deployed data packages. I attached myself to that team because I saw where the future was going and wanted to make sure, I kept up and had a good career."

That decision set him on a lifelong path of technical curiosity and leadership. He eventually led teams that deployed mobile data networks, gaining early experience in how to secure environments and keep operations running under pressure. "I took a liking to security concepts including different ways of securing an environment, physical and logical, keeping bad people out, and allowing people on site to do what they need to do," he says.

After leaving active duty, Michael started his own company before moving into defense contracting in San Diego, supporting the Navy and various Department of Defense entities. "There's a big footprint here for DoD contractors," he says. "From there I joined as a government employee running the NMCI network as the lead engineer, and later moved to the private sector to do product security for Teradata."

When the pandemic hit, he pivoted again, this time leading pre-sales engineering for a security vendor. During that period, he conducted a cybersecurity assessment for Neurocrine Biosciences. "The CIO liked what I was doing and what I delivered," he recalls. "That was that, I moved over to the Chief Information Security Officer position."

BECOMING A BUSINESS LEADER

Michael quickly realized that being a CISO required both technical depth and business and leadership skills. "There are some skill sets that map well like critical thinking, storytelling, and the ability to condense very technical concepts to a non-technical audience," he explains. "But there were other aspects I wasn't aware of at the time, mainly around legal and compliance for Biotech."

He also discovered that the expectations for CISOs have evolved far beyond traditional IT. "We have to know finance, we have to know the business, we have to know marketing," he says. "We have to be able to articulate cases and tell stories, not only our cybersecurity capabilities but our acumen as business leaders."

BUILDING A MODERN CYBERSECURITY PROGRAM

Today, Michael oversees all aspects of Neurocrine's cybersecurity program, including data protection, identity and access management, security architecture, engineering, governance, and incident response. "It's the entire cybersecurity program," he says. "We also just christened AI security, which I'm sure everybody's dealing with now."

Security awareness is a major priority for him. Michael views it as a cultural issue rather than a compliance checkbox. "People across the business are very smart, but they don't always know the jargon, the risks, or the impact if something goes wrong," he explains. "My goal is to build a culture where people feel comfortable reporting issues. It's not a punitive thing if something bad happens. We need employees to tell us when something seems off."

Looking to the year ahead, his top priorities are risk management, automation, AI security, and maturing third-party risk. "We're a publicly traded company, so we have to deal with audits just like everyone else," he says. "That can take up a lot of time for engineers and architects. We're focused on automating controls and artifacts so we can

standardize the process. It shouldn't depend on who's in the role, anyone should be able to step in and close out that audit artifact."

Michael is also working to gamify security training. "The punitive approach doesn't work," he says. "We're moving toward a gamified, positive approach with department leaderboards and small competitions. It's about getting people to pay attention and making awareness something they want to be part of."

AI, RISK, AND THE CHANGING LANDSCAPE

Artificial intelligence is one of the most significant challenges facing security leaders today. "AI has hit us all sideways," Michael says. "There's no Cyber AI bachelor's degree coming out of school anywhere. There's no formal training because these things, like Model Context Protocol (MCP), just came into realization last year."

"We're learning about these technologies at the same time as the adversaries," he says. "There's really no getting ahead of it. You just have to stay current and agile."

Regulatory complexity adds another layer of pressure. "We have a lot of uncertainty with what's coming out of the current administration," he says. "There's also the state-level piece, and then the global considerations. It's constantly evolving."

That evolving threat landscape requires a balance between security and innovation. "We want to be secure and take a risk-based approach, but the business wants to move quickly," he says. "If we don't adopt new technologies, it can negatively impact the business, but if we move too fast, that can also create risk. Finding that middle ground is the challenge."

LEADING WITH EMPOWERMENT

Michael's leadership philosophy centers on trust and empowerment and he encourages innovation and continuous learning. "If someone goes off and learns something new, I want them to bring it back to the team," he says. "We can figure out together how to adopt it or modify the idea moving forward."

Mentorship has become one of his most meaningful responsibilities. "Helping others grow in their careers is incredibly rewarding. I might only get to work with someone for a small window of their life, but I want to set them up for success."

When hiring, he looks for curiosity and a hunger to learn. "The biggest thing I look for is eagerness, a person who's hungry to learn, self-taught, and collaborative. Everything else can be trained."

STAYING CONNECTED AND GIVING BACK

Michael stays connected to the cybersecurity community through local and national groups. "Here in San Diego, we have many groups, and a small brain trust of CISOs in biotech that meet once a month for lunch," he says. "We just talk about what's going on." He also participates in national industry networks. "These types of groups offer open communication, message boards, Slack channels, all ways to share what's landing and what isn't."

At Neurocrine Biosciences, Michael leads with the same principles that have guided him from the Army to the C-suite including empowerment, communication, and purpose. "Being a CISO is about more than keeping bad actors out," he says. "It's about helping people do what they need to do safely and creating an environment where security enables innovation instead of limiting it."

PROFILES IN *Confidence*

ROSE LALLY

CISO

Altisource

Headquarters: Luxembourg

Employees: 1,1,60

Annual Revenue: $150.4 Million

Rose Lally's career began long before cybersecurity was a defined discipline. Her first job out of college was at IDX, where she worked as a programmer and was introduced to a tool called Security Plus. "It was the first inkling of anything related to cybersecurity," she says. "We would probably equate it today to more of an identity and access management tool, but that's where I started getting into the concept of people having role-based access or layered security on personal data."

When HIPAA regulations were introduced, Rose led a new ecommerce team focused on healthcare privacy and data security. "We converted people from those big magnetic tapes to electronic data interchange," she recalls. Her company was later acquired by GE, where she held multiple leadership roles that shaped how she approaches management today. "GE has this concept where they take leaders they think have potential and drop them into individual contributor roles for a year," she explains. "You learn to influence people who don't report to you, how to use metrics and KPIs, and how to present to executives who don't have to take your advice." That experience proved invaluable when she transitioned into infrastructure leadership, providing data center services for hospitals and universities, especially when she launched disaster recovery services soon after Hurricane Katrina struck.

Seeking to broaden her expertise, Rose then spent several years at a global manufacturing company, overseeing all technology services, security, and vendor management and was ready for new challenge. "My cousin called and said, 'There are several open positions I think you'd be a great fit for, and you'd really like this company and its culture,'" she recalls. That company was Altisource. "I went in for an interview and opted for governance and controls - a new team being formed to oversee the technology organization as emerging regulations around data privacy and security took shape. I've always enjoyed building teams from the ground up to tackle new challenges and have a deep interest in all things risk."

It didn't take long for her role to expand. "Through building that team, we uncovered opportunities to strengthen security controls, and eventually I was asked to lead InfoSec - becoming CISO about seven years ago."

A CULTURE OF SUPPORT

Rose has stayed at Altisource longer than most CISOs remain in a single role, and she credits that to a culture of trust and support. "I report to our CTO/Chief Strategy Officer," she says. "He's the same person who hired me, and he always has my back, provides unwavering support and insightful guidance. That kind of support is rare."

Her tenure has also been shaped by consistency within leadership. "I've been working with the same leadership team for about ten years," she says. "We got through COVID together and all the craziness that came with it. Many of my direct reports have been with me for years, and that strong foundation of mutual respect and trust goes a long way in retaining great colleagues."

That longevity, she says, builds trust that can't be replicated. "Every day is something different, and there's no playbook because it's unprecedented," she says. "The support I receive for my decision-making is at the base of our loyalty and commitment - key elements of a stable and resilient leadership environment. Why would I go anywhere else?"

LEADING COMPLEX PROGRAMS

Rose oversees governance and controls, information security, business continuity and disaster recovery, IT asset management, technology risk, corporate vendor management, and even facilities. "Bringing these areas together under my

leadership was driven by the need for a unified approach to risk management - strengthening resiliency, enhancing security, and ensuring robust governance across technology and physical domains."

With such a broad scope, she relies on collaboration and strong teams. "It's a lot," she admits, "but I wouldn't be able to do it without my team and the support of leadership." She describes how consolidation has helped streamline decision-making. "Before, I'd have to join calls with four or five other leaders and we'd all be debating from our own perspectives. Now those conversations are with my direct reports, and we're invested in figuring things out together. It's much more collaborative."

AI, RISK, AND HUMAN ERROR

Looking ahead, Rose is focused on three major priorities: artificial intelligence, third-party risk, and minimizing human error. "I'm a big fan of AI for productivity and efficiency, but I'm also a little terrified of it," she says. "I know all the risks, and I try to stay educated on the regulations and threats that come with it."

She believes AI can be both a solution and a vulnerability. "AI offers immense potential for productivity and efficiency, but it requires strict governance. Our approach is proactive - implementing safeguards to ensure responsible and secure adoption."

To encourage learning, Rose created an internal education series called Knowledge and Nibbles, a play on "lunch and learn" where global employees share short presentations on how they use AI. "We have people from all over the company do 5 to 7 minute sessions on how they're using AI to make their work easier," she says. "At the same time, I sneak in education on security, how to use AI safely while still exploring its benefits."

While AI is top of mind, she's equally focused on people. "Human factors are the number one challenge," she says. "You can have world-class security tools, but unintentional human errors can undermine everything." She often uses a car analogy: "Accidents happen, which is why most vehicles are equipped with safety features - many operating behind the scenes - to help keep drivers and passengers safe."

BUILDING AWARENESS AND TRUST

Rose's approach to leadership includes consistent education and open communication with business leaders. "I use data to show leaders what's really happening," she says. "When I was working on phishing awareness, I used a gamified tool that gave scorecards. I'd present how each team performed, and it turned into a competition. Suddenly, everyone was invested."

That hands-on, visual approach has proven powerful. She recalls using an AI-generated voice phishing simulation to make risk more tangible. "It was the CEO's voice on the call telling people to reset their passwords," she says. "As they said no, the voice got more urgent. It took a minute and a half to make people realize how real this is and the damage that could be done."

She also keeps executives informed whenever major industry incidents occur. "If a vendor has a breach, I'll share the details to the CEO and his leadership team," she says. "I'll say, 'Our customers might ask about this. Here's how we're protected.' It not only builds trust but also ensures future conversations are grounded in awareness of emerging issues."

LEADERSHIP AND LIFELONG LEARNING

Rose describes her leadership style as transparent and supportive. "I can't be successful unless my teams are," she says. "I rely on people's strengths, offer training where it's needed, and ask for feedback regularly. I want to know what's driving them crazy, what I can do differently, and how I can best support them."

She emphasizes empathy and balance. "I meditate every morning," she says. "It helps me start the day calm, and to make a concerted effort every day to treat people the way I want to be treated. If someone calls me for help, I do my best to get them to the right person or solve it myself."

Her team spans multiple functions, and she takes pride in their growth. "Most of them have been with me for years, and some have changed roles and areas of expertise a few times – it's a remarkable group of people."

Outside of Altisource, Rose remains active in the cybersecurity community. She attends and speaks at events, often focusing on leadership, risk management, and women in cybersecurity. "If it's about women in tech or leadership, I usually say yes," she says. "It's important to get out there, represent, and show support. I had a very strong woman as a mentor for many years early on in my career – I keep that in mind and do my best to pay it forward whenever I can."

Above all, she believes continuous learning is essential. "I make time every morning to listen to new webcasts or read relevant articles," she says. "Cybersecurity moves fast. You have to stay on top of it and never get complacent."

PROFILES IN *Confidence*

SEAN DOBSON

CISO & CTO
Wafra

Headquarters: New York, NY

Employees: 180+

Assets Under Management: $28 Billion

Sean Dobson's journey to becoming the Chief Information Security Officer and Chief Technology Officer at Wafra is marked by curiosity and a constant drive to learn. His passion for technology began early, sparked by a fascination with how computers worked and a determination to master them. While in college, he led the help desk supporting more than 40,000 students, an experience that offered deep exposure to real-world IT challenges. "I decided I was going to learn everything about computers," Sean recalls. "That curiosity brought me to studying it in college."

One of his first jobs was at Merck, one of the world's largest pharmaceutical companies, which provided a foundation that would shape his technical depth. There, he cycled through numerous roles including web design, Linux administration, storage, and hardware support, earning a reputation as a deeply technical problem solver. Yet while his technical skills flourished, he recognized a gap in his ability to effectively communicate. "My review from that time said I was the most technical person my boss had ever worked with, but that I needed to work on my communication skills."

Determined to strengthen that skill, Sean pursued a master's degree from Stevens Institute of Technology. The program, focused on the intersection of business and technology, transformed his perspective. "It wasn't just about being technical, it was about learning why technology exists in the business," he explains. It also pushed him out of his comfort zone through presentations and public speaking, helping him overcome what he once described as his "worst fear."

After earning his degree, Sean joined Accenture, where he expanded his technical foundation through consulting engagements involving data center migrations, networking, and large-scale storage projects. The role exposed him to executive stakeholders and honed his ability to translate complex technology into business value. From there, he transitioned to the finance sector, helping build infrastructure and security programs for hedge funds. "Once I really started to focus on security, that was all I would think about, even when I wasn't at work. It was during this time I decided to really focus on the security side of things," he says.

When the hedge fund Sean was working at closed during the 2008 downturn, Sean joined another hedge fund and built their security program becoming the Chief Information Security Officer. That hedge fund eventually closed in 2017 when Sean joined a crypto startup called Digital Asset Custody, where he served as CISO and later CTO. "We built the security program, helped build the product, and eventually sold the company," he explains. That success led him to his current position at Wafra, where he now leads both technology and cybersecurity as CISO and CTO. "I handle everything including cyber, infrastructure, helpdesk, development, and automation," Sean says. "It keeps me on my toes. Every day is different."

BUILDING A CULTURE OF INNOVATION

At Wafra, Sean has helped establish a strong, top-down security culture, one where every employee is engaged. His next challenge, he says, is extending that mindset to artificial intelligence. "I created our AI working group about two years ago," he explains. "My biggest focus now is to create an AI culture, pushing AI throughout the organization while making sure it's done securely."

Right now, Sean's three main areas of focus are AI, automation, and data security, which aligns both his technical foundation and his forward-looking leadership. "Around AI, we're focused on observability and posture management," he says. "We want to make sure that as AI expands, we can monitor it, understand it, and secure it." On data security, he sees meaningful progress after years of complexity. "It was

always an impossible problem to solve, but now we're seeing platforms that really help. We can detect if someone tries to upload sensitive data to an AI site, track the context of data across sources, and have a central view into the entire data universe" he notes.

Automation is another key area of focus. "We've probably automated hundreds of processes over the last couple of years," Sean says. "From onboarding and offboarding to our security operations center, we're freeing up people to think, innovate, and move faster."

ENGAGING EXECUTIVES

When it comes to executive communication, Sean emphasizes simplicity and relevance. "When I first started presenting to executives, I came in with a 30-slide deck to show everything we were doing," he admits. "By slide two, they said, 'Just tell me what matters.'" Now, his approach is conversational and concise. "I keep it to two slides. I focus on high-level risks, what we're doing about them, and how we're improving. It's more about dialogue, asking what they're hearing, what they care about, and less about me presenting a list."

His cadence for executive updates depends on the audience, ranging from semi-annual to annual, especially given Wafra's structure as a private equity firm. "Once the trust sets in, it's less about slides and more about meaningful conversations," he explains. "They know we understand the landscape, and that we're continuously improving."

NAVIGATING CHALLENGES

Among current challenges, Sean highlights the evolving complexity of insider threat programs. "Anytime you look for insider risk, you're going to find it," he says. "It's not that people are malicious, but a good example is that they naturally may want to take some of their files they've worked hard on when they leave." Managing that balance, protecting data while maintaining trust, remains a top priority.

He's also focused on scaling cybersecurity support across Wafra's portfolio companies. Depending on the need and relationship it could be anything from advisory to building a program. The goal isn't perfection; it's what Sean calls "basic cyber hygiene."

LEADING WITH TRUST, EMPATHY, AND INTEGRITY

Sean's leadership philosophy has evolved over time, from being a hands-on technologist to a people-first leader. "The turning point for me as a leader was when I decided to fully trust my team," he says. "I let them take things and make mistakes, and it freed me to think strategically."

He describes his leadership style as adaptive and grounded in core principles. "Everyone is different. Some people respond to encouragement, others need a little more structure. But overall, I'd say empathy and integrity are key," he reflects. "Empathy means understanding that people are doing their best, it's about putting yourself in their shoes. Integrity means doing the right thing, even when no one's looking."

He's also intentional about maintaining balance and morale. "We spend so much time at work; if we're not having fun, collaborating, and enjoying what we do, we're doing the wrong thing," he says. Above all, he views his role as one of service: "I always tell my team, I work for you. My job is to make sure you have what you need to succeed, and to shield you from the noise so you can focus."

Ultimately, Sean's approach blends technical excellence with human leadership. "I used to only want to be liked," he says. "Now, I focus on being respected. My job is to guide, support, and protect the team, because they're the ones driving the mission forward."

PROFILES IN *Confidence*

YASH MURALI

CTO
Therabody

Headquarters: Los Angeles, CA

Employees: 400+

Annual Revenue: Private

For Yash Murali, technology has always been a space where curiosity meets creativity. “I’ve always been fascinated by how things work,” he says. “Growing up, I’d take things apart just to see how they fit together.” That same mindset shaped his early career in engineering, where he built systems that merged design, function, and innovation.

His career spanned across private-equity-backed consumer technology and health and wellness—industries that taught him distinct lessons. Private equity taught him how to move fast, consumer technology showed him the importance of design and user experience, and health and wellness taught him that trust is everything.

Before joining Therabody, Yash held several senior technology roles where he led global teams and built scalable digital platforms. “I’ve always loved the challenge of connecting technology with purpose,” he explains. “For me, success is when technology disappears and when it becomes so intuitive that people don’t even realize how much innovation is behind it.”

LEADING AT THE INTERSECTION OF HEALTH AND TECHNOLOGY

When Yash joined Therabody as Chief Technology Officer, he saw an opportunity to merge advanced technology with the science of human performance. “We’re a wellness technology company,” he says. “That means we sit at the intersection of health, science, and innovation. Our job is to make recovery and wellness accessible to everyone, whether you’re a professional athlete or someone who just wants to feel better.”

At Therabody, Yash oversees the company’s global technology strategy from software and connected devices to data analytics, automation, and security. “My team is responsible for building and securing the digital ecosystem that powers our products,” he says. “That includes everything from mobile apps to AI-driven recommendations.”

He approaches his work with the mindset of a product visionary. “Technology has to create value for the business and for the user,” he says. “I focus on how every product, and every data point can help someone move, sleep, or recover better.”

That connection between product and purpose is what keeps him energized. “Our mission isn’t about selling devices, it’s about improving lives through smarter technology,” he says. “Everything we do ties back to that mission.”

INNOVATION THROUGH DATA AND AI

Artificial intelligence plays a central role in Therabody’s innovation roadmap. “AI helps us understand how the body responds to different treatments,” Yash explains. “It allows us to personalize recommendations and make recovery more efficient.”

The company uses AI to analyze sensor data, track behavioral trends, and optimize device performance. “The future of wellness is personalized,” Yash says. “AI helps us connect the dots, from usage patterns to health outcomes, so we can design experiences that adapt to each individual.”

But he is equally focused on doing it responsibly. “Consumers trust us with their data,” he says. “That trust is sacred. We’re very intentional about how we collect, store, and use data. Transparency and security are non-negotiable.”

He often describes AI as a partner to human intelligence, not a replacement. “AI can amplify creativity and accelerate discovery,” he says. “It can make connections we might miss.

But it still takes human empathy and judgment to decide what to do with that information."

That philosophy drives how his teams design and deploy technology. "We use AI as a lens for innovation," Yash says. "But it's not the end goal, it's a tool that helps us serve people better."

BUILDING AND EMPOWERING GLOBAL TEAMS

Yash leads with a philosophy rooted in trust, empowerment, and shared accountability. "My job is to create the conditions for my team to succeed," he says. "That means removing barriers, setting clear goals, and giving people ownership."

He manages a diverse, global team of technologists, engineers, and data specialists. "When you're leading across geographies and time zones, communication becomes everything," he says. "You can't rely on hallway conversations. You have to be intentional about how you share information, set expectations, and build connection."

He believes that culture starts with empathy. "Every person on the team has different motivations," he says. "Some want to innovate, some want stability, some want to grow into leadership. My role is to help them find that path and make sure they know their work matters."

One of Yash's favorite leadership practices is storytelling. "Data tells you what's happening," he says. "Stories tell you why it matters. When I talk to my team or the board, I use both. People remember stories, they remember how they felt about the work."

That approach has earned him the respect of both technical and business leaders. "You can be the smartest engineer in the room," he says. "But if you can't communicate why it matters to the customer, you're missing the point."

ADAPTING FOR THE FUTURE

Like many technology leaders, Yash sees the future of work and leadership evolving rapidly. "The technology will always change," he says. "What doesn't change is the need for adaptability and curiosity."

He encourages his team to embrace experimentation. "It's okay to fail," he says. "If we fail, we do it fast, learn from it, and move forward. The only true mistake is staying still."

Automation and intelligence are key priorities for the years ahead. "We're building a foundation that scales," Yash says. "That means designing systems that can adapt to new technologies, new regulations, and new customer expectations."

He also sees leadership itself changing. "The next generation of leaders will be those who can connect technology, empathy, and business strategy," he says. "A future-proof leader is someone who can navigate uncertainty without losing sight of the mission."

STAYING CONNECTED AND CONTINUOUS GROWTH

Yash is deeply involved in the broader technology and wellness community. He participates in innovation panels, leadership roundtables, and cross-industry collaborations. "It's important to share what we're learning," he says. "Wellness technology is still young. We all benefit when we share insights and best practices."

Continuous learning remains central to his leadership. "I make time to read, listen to podcasts, and learn from my peers," he says. "You can't lead in technology if you stop learning. The moment you think you've figured it out, you're already behind."

He encourages his teams to do the same. "We have to model the curiosity we expect," he says. "If I'm learning something new every day, my team sees that and follows suit."

At Therabody, Yash's leadership is defined by balance with innovation and integrity, data and empathy, technology and humanity. "We're using technology to improve people's lives," he says. "That's what keeps me excited. Technology is only powerful when it helps people feel better, move better, and live better."

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM